

Abstract

An MKB and a device key 121 of a drive are input to a process MKB 122. The process MKB 122 performs a revoking process for the drive. A process MKB 132 performs a revoking process for a host 103. The host 103 compares MAC values calculated by MAC calculating blocks 123 and 133. When the host 103 has determined that the two values are the same, the host 103 has successfully authenticated the drive 102. The drive 102 compares MAC values calculated by MAC calculating blocks 134 and 124 of the host 103. When the drive 102 has determined that the two values are the same, the drive 102 has successfully authenticated the host 103. When the mutual authentication has been successfully performed, the MAC calculating blocks 125 and 135 generate a common session key.